Interdisciplinary Description of Complex Systems 17(1-A), 7-12, 2019

APPLYING RISK MANAGEMENT PROCESS IN CRITICAL INFRASTRUCTURE PROTECTION

Maria Luskova* and Zdenek Dvorak

University of Zlin, Faculty of Security Engineering
Zlin, Slovakia

DOI: 10.7906/indecs.17.1.2
Regular article

Received: 18 June 2018.
Accepted: 31 December 2018.

ABSTRACT

Critical Infrastructure is an asset or system whose disruption or destruction should have adverse effect on the performance of economic and social functions of the state, and thus on the quality of life of residents in terms of the protection of their life, health, security, property, as well as the environment. Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of all developed countries. The Slovak Republic has already adopted some legal standards and measures emphasizing the importance of critical infrastructure issues and aiming at ensuring the required level of its security and protection.

The article deals with the tasks and competences of state administration authorities in the area of critical infrastructure and the obligations of the operators in the protection of the critical infrastructure element in the Slovak Republic. It provides also a framework, application of risk management process as a foundational concept for processing security plan, designed to protect the element of critical infrastructure from disruption and destruction. In conclusion it emphasizes the need of close cooperation between public and private sectors to ensure proactive approach to securing critical infrastructure.

KEYWORDS

critical infrastructure, security, resilience, security plan, risk management

CLASSIFICATION

JEL: H12, H84, J28

*Corresponding author, *η*: maria.luskova@fbi.uniza.sk, +421 41 513 6766;
Univerzitna 8215/1, 010 26 Žilina, Slovakia

INTRODUCTION

Over the last twenty years technologically developed countries give increased attention to the question of the critical infrastructures protection (CIP). New threats, the dynamical development of technologies, continuous changes in the politics and economics increase the need to search for more effective ways to protect people, property and environment, situated in the certain area.

European Council Directive 2008/114/EC [1] defines a concept of the European Critical Infrastructures (ECI), which became the basis for the way of identifying the most important elements of national infrastructure in the different countries of the European Union. For simplicity, it is possible to state that the ECI is s a set of the most important elements of the national critical infrastructures each of the concerned countries.

The critical infrastructure (CI) is the part of national infrastructure; i.e. selected information systems, services, organizations, and their important objects and facilities; whose destruction or disruption, as a consequence of its exposure to certain risk factor, will cause a danger or disturbance in the society functioning or threat to life and health of the citizens. In fact, the particular system or service will be considered as a potential CI element if it will fulfill the significant role for some sector which can significantly affect security.

CIP is very actual topic. The involved countries had progressively established a legal framework of CIP on the national base (e.g. in Slovakia it is Act No. 45/2011 Coll. on Critical Infrastructure, in the Czech Republic it is the Act No. 240/200 Coll. on Crisis Management, in Poland it is document The National Critical Infrastructure Protection Programme). It can be stated that critical infrastructure is in developed economics part of the security system of the state.

For a correct understanding of CI it was necessary to define list of critical infrastructure sectors. In the most countries involved in the European Programme for Critical Infrastructure Protection (EPCIP), the major European sectors of CI are:

- energy (electricity, gas, oil industry, mining),
- information and communication technologies (satellite communication, networks, data centers, sources of classified information, control and information systems of infrastructures, etc.),
- transport (road, rail, air and water).

added with other areas important to the society functioning, such as the provision of drinking water, food security, financial sector, infrastructure of medical equipments and others.

CRITICAL INFRASTRUCTURE IN SLOVAKIA

The Slovak Republic (SR) as a member of the European Union participates in development of documents concerning the CI and especially their incorporation into legislative framework. At present, the issues of CI in the SR are codified in the act No. 45/2011 Coll. of 8 February 2011 on Critical Infrastructure (hereinafter Act) [2]. The Act provides the organization and competence of state administration authorities in the area of CI, the procedure for designating elements of CI and the obligations of the operator in the protection of the CI element and liability for breach of these obligations. CI includes a defensive infrastructure under a special regulation. Administration in the field of CI is performed by the Government of the SR, Ministry of the Interior of the SR and Ministries indicated in Table 1. Their competences as well as the obligations of the CI operators are defined by the Act. In the SR the CI sectors under the competences of central authorities are defined in Table 1.

Table 1. Critical Infrastructure Sectors under the competence of central authorities [2].

Sector	Sub-sector	Central authority
1. Transport	Road transport Aviation transport Water transport Railway transport	Ministry of Transport, Construction and Regional Development of the Slovak Republic
2. Power industry	Mining Electrical Energy Gas industry Oil and oil products	Ministry of Transport, Construction and Regional Development of the Slovak Republic
3. Information and communication technologies	Internet Information systems and networks	Ministry of Economy of the Slovak Republic
4. Electronic communications	Satellite communication Networks and services of stable and mobile electronic communications	Ministry of Finance of the Slovak Republic
5. Post	Providing postal services, post system of payments and administering activities	Ministry of Transport, Construction and Regional Development of the Slovak Republic
6. Industry	Pharmaceutical industry Metallurgical industry Chemical industry	Ministry of Economy of the Slovak Republic
7. Water and atmosphere	Providing drinking water Water buildings Meteorological service	Ministry of the Environment of the Slovak Republic
8. Health Services	N.A.	Ministry of Health of the Slovak Republic

Important documents except of the current version of Act No. 45/2011 Coll. on CI, related to the protection of critical infrastructure in Slovakia are, in particular, the National Program for Protection and Defense of CI in the SR, the Concept of Critical Infrastructure in the SR and related Act No. 319/2002 Coll. on Defense of the SR, Act No. 261/2002 Coll. on Prevention of Serious Industrial Accidents, the National Action Plan for Combating Terrorism, Act No. 129/2002 Coll. on Integrated Rescue System, Act No. 387/2002 Coll. on Management of State in Crisis Situations Other Than Time of War and State of War, and other [3].

OBLIGATIONS OF OPERATORS

The responsibility for protecting and defending critical infrastructure in the SR holds the public administration together with the owners and operators of the CI elements.

An important part of the law is the formulation of basic duties of operators of CI elements. Operators are required to take all necessary measures to protect the CI element and thereby ensure its functionality, continuity and integrity of the element's activities in order to prevent, avert or mitigate threats of disruption or destruction.

Significant aspects in relation to the operator's obligations include:

- developing and updating the operator's security plan,
- practicing a model situation of a threat of disruption or destruction of the element according to the security plan at least once every three years,
- designating an authorised person who is also the contact person relating to an element of the European Critical Infrastructure,
- providing assistance to the competent central authority, especially data, documents and explanations necessary to:

- designate the element and its inclusion in the sector, as well as the removal of the element from the sector,
- assessment of the protection of the element, including ensuring protection of the element by the operator of the security service or armed security team,
- prepare a risk analysis of the sector,
- manage the registry of elements.

RISK MANAGEMENT AND PROCESSING THE SECURITY PLAN

Security plans are a tool to increase the security of critical infrastructure elements. Minimum procedure in the processing of the security plan is formulated in the Annex 2 of the Act No. 45/2011 Coll. on Critical Infrastructure and indicated in Figure 1.

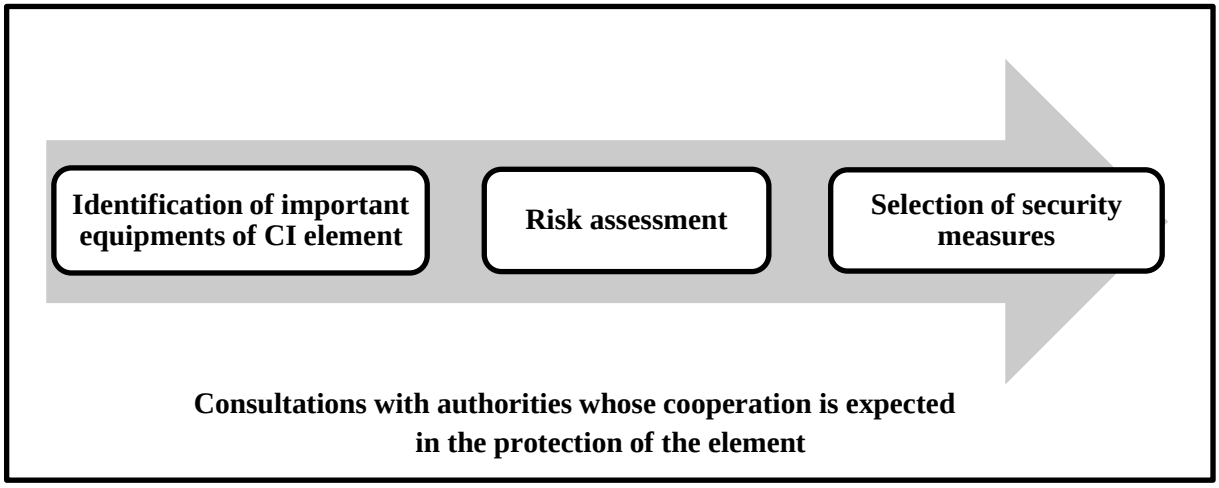

Figure 1. Minimum procedure in the processing of the security plan.

Minimum procedure in the processing of the security plan is closely related to the risk management process defined by ISO 31000:2009 which provides principles and generic guidelines on risk management. Relation between risk management process and processing the security plan is indicated in Figure 2. In this context, the individual steps of the security plan development can be described as follows:

- *Identification of important equipment of the CI element* – this phase relates to the analysis of the internal security environment of the critical infrastructure element. It aims to ensure reliable, up-to-date and relevant information on the situation and the state of the internal security environment, with emphasis on the threats needed to identify security risks. It includes an inventory of significant assets, in which it is necessary to include also the premises and objects of the whole organization, as well as significant assets, located in the individual spaces inside the buildings, which are called protected areas.
- *Risk assessment* – the overall risk identification process, risk analysis and risk assessment. When assessing the risks, the following key questions need to be answered:
  - What can happen and why?
  - What are the consequences?
  - What is the likelihood of their further occurrence?
  - Are there any factors that mitigate the risk consequences or reduce the risk likelihood?
  - Is the level of risk tolerable or acceptable and requires further treatment?

  Risk assessment allows managers and stakeholders to better understand the risks that could affect the achievement of objectives, their causes, consequences and the likelihood and effectiveness of risk management measures
- *Selection of security measures* – this stage applies to risk treatment. Risk treatment focuses on those risks that were not considered acceptable, i.e. their value is above the

acceptability limit. It consists of designing, adopting and implementing measures that influence their value in a selected way. Risk treatment methods may not necessarily be mutually exclusive or may not be appropriate in all circumstances. Risk treatment may create new risks or modify existing risks [4].

- *Consultations with the authorities, whose cooperation is expected in the protection of the element* – this stage covers communication and consultation as well as monitoring and review.

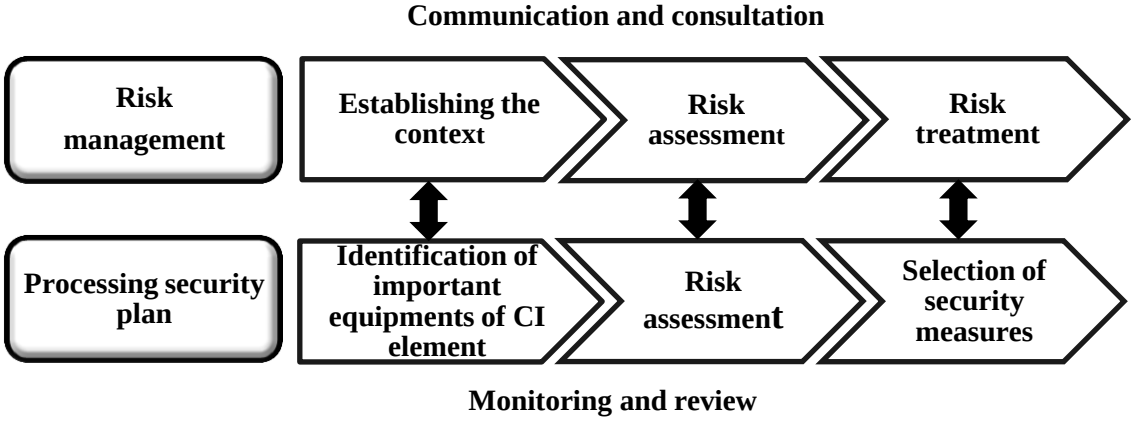

Figure 2. Relation between risk management process and processing the security plan.

Communication and consultation with external and internal stakeholders take place during the whole process of the security plan development. It is important that the staff responsible for the element protection and the stakeholders understand on what basis the decisions are taken and also to understand the reasons why certain activities are required.

Monitoring and review must include regular surveillance and periodic inspections, which may be periodic or ad hoc. Their goal is, e.g. to achieve more information to improve risk assessment, analyse events and learn from them, identify emerging risks, etc.

Risk management needs to be a continuous process since in day-to-day operations, incidents can undermine the best-laid plans and best-of-breed technologies [5, 6]. Security plans are a tool to increase the security of critical infrastructure elements. Their structure and scope is also formulated in Annex II of Council Directive 2008/114/EC. Together with the set of system measures of all actors involved in the management of the CI element and the intrinsic capabilities or properties of the element naturally resist the external and internal effects of the environment; they create conditions for achieving the resilience of the CI element [7, 8].

CONCLUSION

More than 90 % of CI in the SR is owned by private sector. It is evident that security cannot be just the responsibility of government but both the public and private sectors should work closely to adopt a more proactive approach to securing critical infrastructure. Close cooperation and exchange of information between all stakeholders is necessary to take into account the interdependencies between the CI elements and to identify the impact at the system level. It is important for owners and operators of CI to prefer the protection of critical infrastructure elements in terms of a safety and security to an economic point of view.

ACKNOWLEDGEMENTS

Preparation of this article was supported by the European Union within the FP7 project No. 608166 “Risk Analysis of Infrastructure Networks in response to extreme weather” and by VEGA grant No. 1/0240/15 “Process model of critical infrastructure safety and protection in the transport sector”.

REFERENCES

[1] Council of European Union: *Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection*.
http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:01:EN:HTML, accessed 8th March 2018,

[2] –: *Act No. 45/2011 Coll. about critical infrastructure*.
http://www.zbierka.sk, accessed 8th March 2018,

[3] Hromada, M.: *Technological aspects of CIP in Slovak CI*. Ph.D. Thesis.
University of Zlin, Zlin, 2011,

[4] Leitner, B.: *General model for railway systems risk assessment with the use of railway accident scenarios analysis.*
Procedia Engineering **187**, 150-159, 2017,
http://dx.doi.org/10.1016/j.proeng.2017.04.361,

[5] Luskova, M. and Buganova, K.: *The importance of effective risk management system in the Slovak enterprises.*
WMSCI 2011 – The 15th world multi-conference on systemics, cybernetics and informatics. Orlando, International Institute of Informatics and Systemics, 2011,

[6] NTTSecurity: *Risk management is a continuous process.*
https://insight.nttsecurity.com/post/102dhyq/risk-management-is-a-continuous-process, accessed 8th March 2018,

[7] Hromada, M. et al: *System and way of critical infrastructure resilience assessment*.
UTB, Zlín. 2013,

[8] Rehak, D. et al: *European Critical infrastructure risk and safety management. Directive implementation in practice*.
Chemical Engineering Transactions **48**, 943-948, 2016,
http://dx.doi.org/10.3303/CET1648158.